WHAT IS CLAIMED IS:

1. A method for using a binary state machine for processing a data stream in an intrusion detection system, the method comprising:

maintaining a state table, the state table indexed such that inputs comprising a current state and a current character yield an output of a new state, the new state related to an indication of an attack on a computer network;

maintaining the current state;

receiving an input stream, the input stream comprising a plurality of characters;

selecting a first character of the input stream as the current character; and

comparing a current character and the current state to the state table to generate a new state.

2. The method of Claim 1, further comprising initializing the current state to an initial state.

3. The method of Claim 1, further comprising:

setting the current state equal to the new state;

selecting a next character as the current character, the next character appearing subsequent to the first character in the input stream; and

repeating the comparing step.

4. The method of Claim 1, further comprising recognizing the new state as indicative of an attack upon the computer network.

a6 con't

5. The method of Claim 5, further comprising sounding an alarm.

6. The method of Claim 1, further comprising generating the state table from a REGEX command.

A6 cont

7. A system for use as a binary state machine for processing a data stream in an intrusion detection system, the system comprising:

a state table indexed such that inputs comprising a current state and a current character yield an output of a new state, the new state related to an attack on a computer network; and

a state machine communicatively coupled to the state table, the state machine operable to:

maintain the current state;

receive an input stream, the input stream comprising a plurality of characters;

select a first character of the input stream as the current character; and

compare the current character and the current state to the state table to generate a new state.

8. The system of Claim 7 further comprising a computer readable medium, wherein the state table is stored upon the computer readable medium.

9. The system of Claim 8, wherein the state machine comprises software code stored upon the computer readable medium, the software code further operable to be executed by a computer processor.

10. The system of Claim 7, wherein the state machine is further operable to initialize the current state to an initial state.

a6 cont

11. The system of Claim 7, wherein the state machine is further operable to:

setting the current state equal to the new state;

selecting a next character as the current character, the next character appearing subsequent to the first character in the input stream; and

repeating the comparing step.

12. The system of Claim 7, wherein the state machine is further operable to recognizing the new state as indicative of an attack upon the computer network.

a6 cont

13. A system for use as an intrusion detection system, the system comprising:

a computer readable medium;

a network interface for receiving an input stream comprising a plurality of characters;

a processor communicatively coupled to the computer readable medium and the network interface;

a state table stored upon the computer readable medium, the state table indexed such that inputs comprising a current state and a current character yield an output of a new state, the new state related to an attack on a computer network; and

a state machine comprising instructions stored upon the computer readable medium and executable by the processor, the state machine communicatively coupled to the state table, the state machine operable to:

maintain the current state;

select a first character of the input stream as the current character; and

compare the current character and the current state to the state table to generate a new state.